Configuring ATM Half-Bridge Services

BayRS Version 12.10
Site Manager Software Version 6.10

Part No. 300017-A Rev. 00
February 1998

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. February 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

BCN, BLN, BN, FRE, GAME, Optivity, PPX, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, BCC, BCNX, BLNX, IP AutoLearn, PathMan, RouterMan, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software productmay be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Before You Begin xiii
Conventions xiv
Acronyms xv
Bay Networks Technical Publications xvi
Bay Networks Customer Service xvii
How to Get Help xvii
Bay Networks Educational Services xviii

Chapter 1
ATM Half-Bridge Overview

What Is ATM Half Bridge? 1-1
How the AHB Router Works 1-4
Forwarding Inbound Packets from CPE Hosts 1-4
Forwarding Outbound Packets to CPE Hosts 1-5
Using DHCP to Dynamically Assign IP Addresses 1-5
Dynamically Learning New Bridge Table Entries 1-7
Unsecure Learning Method 1-8
Secure Learning Method 1-8
Maintaining the AHB Bridge Table 1-9
Adding Bridge Table Entries 1-9
Removing Bridge Table Entries 1-10
Replacing Bridge Table Entries 1-10
Using Source-Based Routing 1-10
Responding to Proxy ARP Requests 1-11
Using Inbound Packet Filtering 1-12

Chapter 2
Starting AHB Services

Network Planning Considerations 2-1
AHB Configuration Requirements 2-1
Preparing a Configuration File 2-2
Configuring an IP Interface on the Router 2-3
Configuring Circuitless IP on the Router 2-4
Configuring AHB Services 2-5
Creating an ATM Interface 2-6
Adding an LLC/SNAP PVC Service Record 2-6
Adding AHB to the LLC/SNAP Service Record 2-7
Adding PVCs to the LLC/SNAP PVC Service Record 2-9
Configuring a DHCP/BootP Relay Agent 2-10
Creating a BootP Relay Agent Forwarding Interfaces 2-10
Configuring BootP Preferred Servers 2-12
Specifying the Relay Agent IP Address 2-12
Specifying the Target Server IP Address 2-13

Chapter 3
Customizing AHB Services

Modifying the AHB Configuration 3-1
Enabling and Disabling AHB 3-1
Setting the Auto Learn Method 3-2
Configuring a Local AHB Init File 3-3
Sample Init File 3-3
Specifying an Alternate Init File 3-5
Specifying the Debug Level 3-6
Enabling and Disabling Inbound Packet Filtering 3-7
Modifying AHB Circuits 3-8
Enabling and Disabling an AHB Circuit 3-8
Specifying the Subnet Mask for the Learned Host 3-9
Enabling and Disabling Proxy ARP on a Circuit 3-10
Configuring Traffic Filters for Source-Based Routing 3-10
Deleting AHB from the Router 3-11

Appendix A
AHB, BootP/DHCP, IP, and ATM Parameter Descriptions

AHB Global Parameters A-2
AHB Circuit Parameters A-6
BootP Relay Agent Interface Table Parameters A-8
BootP Address Parameters A-10
BootP Relay Agent Preferred Server Table Parameters A-12
BootP Preferred Server Configuration Parameters A-14
IP Configuration Parameters A-15
ATM Interface Parameter Descriptions A-17
ATM Service Record Parameter Descriptions A-19
ATM Virtual Channel Link Parameter Descriptions A-23

Appendix B
Understanding ATM Concepts

ATM General Information B-1
ATM Cells B-1
Cell Headers B-1
ATM Data Transmission B-3
Permanent Virtual Connections B-5
Service Records and Virtual Circuits B-5
Data Encapsulation B-5
Assigning a Data Encapsulation Type for a PVC B-6
PVC Access Methods B-6
Multiple PVCs B-7
One PVC B-8

Figures

Figure 1-1. DSL Network with an AHB Router 1-3
Figure 1-2. How CPE Hosts Identify a DCHP Server 1-6
Figure 1-3. How CPE Hosts Request and Receive IP Addresses from the DHCP Server 1-7
Figure A-1. Edit ATM Half-Bridge Global Parameters Window A-2
Figure A-2. ATM Half-Bridge Circuit List A-6
Figure A-3. BOOTP Relay Agent Interface Table Window A-8
Figure A-4. BOOTP Addresses Window A-10
Figure A-5. BOOTP Relay Agent Preferred Server Table Window A-12
Figure A-6. BOOTP Preferred Server Configuration Window A-14
Figure A-7. Interface Attributes Window Sequence A-17
Figure A-8. Service Attributes Window Sequence (PVCs) A-20
Figure B-1. ATM Cell B-2
Figure B-2. ATM Transmission Components B-4
Figure B-3. Multiple PVCs per Service Record B-7
Figure B-4. One PVC per Service Record B-9

Tables

Table 1-1. Sample AHB Bridge Table 1-9

About This Guide

If you are responsible for configuring ATM Half-Bridge services, you need to read this guide.

If you want to	Go to
Learn about ATM Half-Bridge concepts and the Bay Networks® implementation of ATM Half Bridge	Chapter 1
Start ATM Half Bridge on a BLN® or BCN® router using default configuration parameter values	Chapter 2
Customize ATM Half-Bridge parameter settings	Chapter 3
Obtain information about ATM Half Bridge, BootP/DHCP, IP, and ATM parameters (this is the same information you obtain using Site Manager online Help)	Appendix A
Learn about basic ATM concepts and terminology	Appendix B

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network).*

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to the *BayRS Version 12.10 Document Change Notice*.

Conventions

bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

AAL	ATM adaptation layer
ADSL	asymmetric digital subscriber line
AHB	ATM Half Bridge
ARE	ATM Routing Engine
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
ATU-C	ADSL terminal unit, central
ATU-R	ADSL terminal unit, remote
AUI	Attachment Unit Interface
BootP	Bootstrap Protocol
BRI	Basic Rate Interface
CO	central office
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
CPE	customer premise equipment
DSLAM	DSL access multiplexer
DTE	data terminal equipment
GUI	graphical user interface
HDLC	high-level data link control
ILI	Intelligent Link Interface
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	internet service provider
ITU-T	International Telecommunications Union-Telecommunications (formerly CCITT)
LAN	local area network
MAC	media access control
MAU	media access unit
MIB	management information base

MTU	Maximum Transmission Unit
OSI	Open Systems Interconnection
PDU	protocol data unit
PVC	permanent virtual circuit
RIP	Routing Information Protocol
SAP	service access point
SDU	service data unit
SNAP	Subnetwork Access Protocol
STAT	status
SVC	switched virtual circuit
TCP/IP	Transmission Control Protocol/Internet Protocol
UTP	unshielded twisted-pair
VC	virtual circuit
VCI	virtual connection identifier
VCL	virtual channel link
VPI	virtual path identifier
WAN	wide area network

Bay Networks Technical Publications

You can now print technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs*. Find the Bay Networks products for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

Documentation sets and CDs are available through your local Bay Networks sales office or account representative.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Bay Networks Educational Services

Through Bay Networks Educational Services, you can attend classes and purchase CDs, videos, and computer-based training programs about Bay Networks products. Training programs can take place at your site or at a Bay Networks location. For more information about training programs, call one of the following numbers:

Region	Telephone number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 282 when prompted 978-916-3460 (direct)
Europe, Middle East, and Africa	33-4-92-96-15-83
Asia/Pacific	61-2-9927-8822
Tokyo and Japan	81-3-5402-7041

Chapter 1
ATM Half-Bridge Overview

This chapter provides an overview of basic ATM Half-Bridge concepts and the specific ways Bay Networks implements these concepts on BLN® and BCN® routers.

This chapter assumes that you understand ATM concepts and terminology. For a brief overview of ATM, see Appendix B. For detailed information about ATM, refer to *Configuring ATM Services*.

This chapter contains information about the following topics:

Topic	Page
What Is ATM Half Bridge?	1-1
How the AHB Router Works	1-4

What Is ATM Half Bridge?

ATM Half Bridge (AHB) is a protocol operating on BLN and BCN routers that connects remote hosts (PCs and workstations) attached via digital subscriber line (DSL) devices (modems) to an IP routed network. These modems send and receive IP packets over ATM PVCs using RFC 1483 SNAP/LLC encapsulation. AHB converts RFC 1483 bridge frames containing IP packets to unencapsulated routed frames and performs the reverse function for packets returning from the opposite direction.

Bay Networks designed AHB to meet the requirements of public network providers who want to develop an end-to-end solution using DSL to provide high-speed internet and remote LAN access to ISP's and corporate networks. The AHB router supports the public network provider's WAN infrastructure network by performing the bidirectional conversion of RFC 1483 Ethernet bridged packets for IP routing to and from the ISP and corporate networks.

Figure 1-1 shows a sample DSL access network that uses an AHB router. This network is divided into four separate segments:

- The customer premises, which consist of the remote host and modem, referred to as ADSL terminal unit, remote end devices (ATU-R)
- The network provider POP, which consists of DSL access multiplexor ADSL terminal unit, central devices (DSLAM ATU-C), ATM access network, and the AHB router
- The public network WAN infrastructure (typically IP over ATM or frame relay)
- The ISP or corporate network, which provides internet service for remote CPE stations

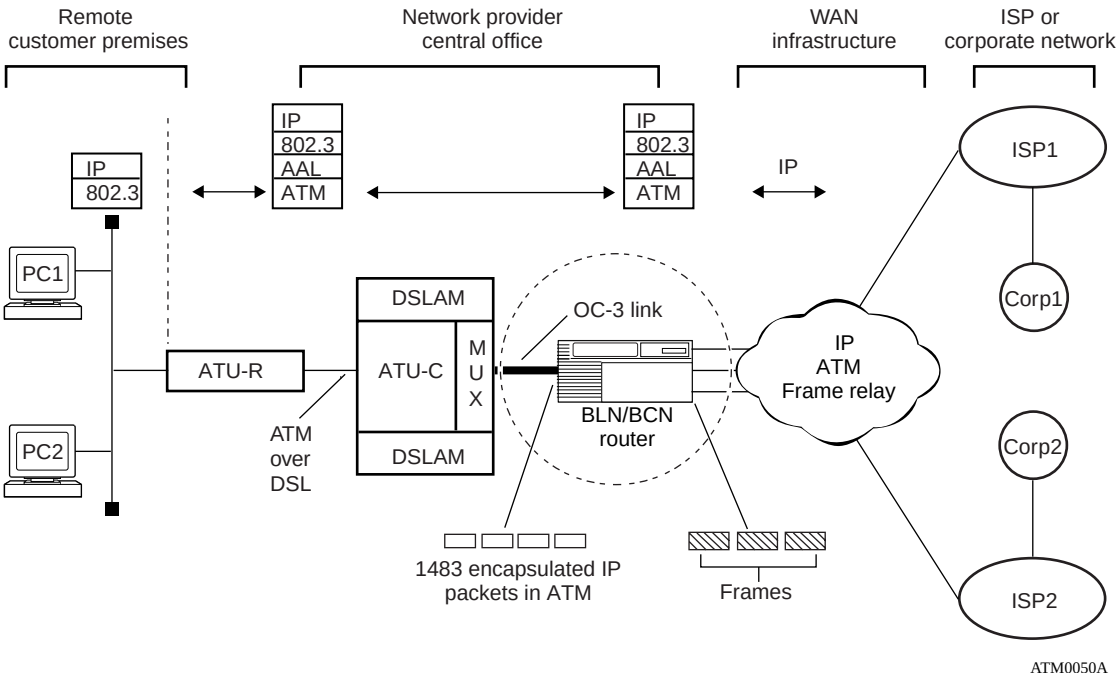


Figure 1-1. DSL Network with an AHB Router

The following steps explain how IP packets travel from the CPE host (remote user) on an Ethernet segment to the AHB router located at the public network provider's central office:

1. A user (PC or workstation) at a remote site sends Ethernet packets to an ATU-R attached to a remote Ethernet LAN segment (10 MB).
2. The ATU-R, acting as an Ethernet/ATM bridge, performs the following tasks:
   - Accepts the Ethernet packets
   - Segments the Ethernet packets into ATM cells according to RFC 1483 (802.2/LLC bridge encapsulation)
   - Transmits the ATM cells to a DSLAM ATU-C at the public network provider's site
3. The ATU-C receives the ATM cells, which are multiplexed along with cells from other ATU-Cs, and transmits them to the ATM network over one or more OC-3 links.

4. The ATM network, located at the central office, switches the ATM cells and forwards them over PVCs to the ATM interface on the AHB router.

How the AHB Router Works

AHB combines bridging and IP routing on the router platform. On the DSL access side, the router receives RFC 1483 encapsulated bridged Ethernet frames containing IP packets from CPE hosts. On the WAN side, ISP's and corporate networks receive routed IP frames. AHB dynamically learns the association between IP addresses assigned to CPE hosts and the correct RFC 1483 bridged Ethernet header data for the host.

Forwarding Inbound Packets from CPE Hosts

AHB decapsulates and then routes IP packets it receives from a remote CPE host to an ISP or corporate network. When AHB receives the incoming packets on its ATM interface, it checks its local bridge table to determine whether the packet's source IP address corresponds to the host IP address in the associated AHB table entry. If the bridge table contains the bridge entry, and the entry matches the bridge information (the correct circuit and VCID), then AHB strips off the RFC 1483 bridged Ethernet header information and forwards the packet using IP routing to the appropriate ISP's and corporate networks.

If AHB does not find the bridge entry in its local bridge table, and you selected unsecure learning mode, AHB creates a new bridge entry using the packet header data from the incoming packet. If you selected secure learning mode, AHB creates a new bridge entry only if this is a new DHCP request (for information about using unsecure and secure learning mode, see "Dynamically Learning New Bridge Table Entries"). The AHB router cannot use this bridge entry until it receives a DHCP reply on a non-AHB interface that matches the destination MAC address in the bridge entry. The IP address is assigned at this time. If no matching bridge entry is found for an incoming packet on an AHB interface, the packet may still be forwarded if either it is a DHCP packet or if you have disabled inbound packet filtering.

Forwarding Outbound Packets to CPE Hosts

IP packets received from ISP's or corporate networks that are destined for CPE hosts are sent to AHB based on the AHB route in the IP routing table. When AHB receives IP packets, it searches its local bridge table for an associated bridge entry based on the packet's destination IP address. If AHB finds an associated bridge entry, it adds the RFC 1483 encapsulation and Ethernet header information to the packet. Then it forwards the packet on the correct outgoing interface and PVC to reach the remote CPE host.

If AHB does not find an associated bridge entry for the packet in its bridge table, it drops the packet.

Using DHCP to Dynamically Assign IP Addresses

CPE hosts can use DHCP to obtain their IP address and default gateway address. When you boot the router, the CPE host sends a DHCP request packet, which is relayed by the DSL modem to the AHB router. The AHB router acts as a DHCP/BootP relay agent. When the BootP relay agent configured on the ATM service record receives the DHCP request packet, it fills in the associated IP interface address (the address you specified for the ATM interface) as the gateway address. The BootP relay agent then forwards the packet to the DHCP server using either the BootP forwarding interface method or the BootP preferred server method.

When the DHCP server receives the DHCP REQUEST packet, it checks to see whether the gateway address is filled in. If this address is filled in, DHCP sends a reply packet (DHCPACK) to the BootP relay agent on the AHB router. The AHB router then forwards the DHCPACK reply to the CPE host using the associated IP address of the unnumbered IP interface.

DHCP servers often use the gateway address in the DHCP request to determine the address pool to use when assigning a client IP address.

The DHCP server may not respond if it receives a DHCP request where the gateway address is on the same subnet as the DHCP server's IP address. Therefore, when selecting an associated IP address for the unnumbered ATM circuit, choose an address other than the IP address of a directly connected DHCP server.

Figure 1-2 shows how the remote hosts identify the DHCP server on the network.

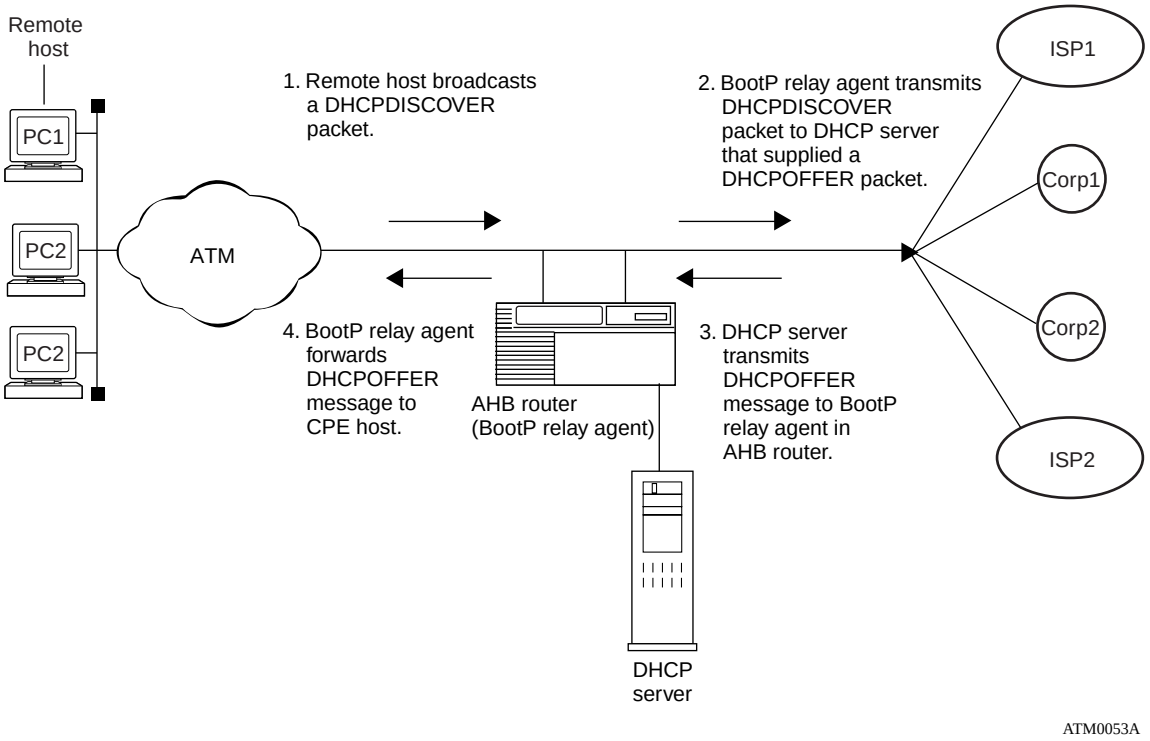


Figure 1-2. How CPE Hosts Identify a DCHP Server

Figure 1-3 shows how the CPE hosts request and receive IP addresses from the DHCP server.

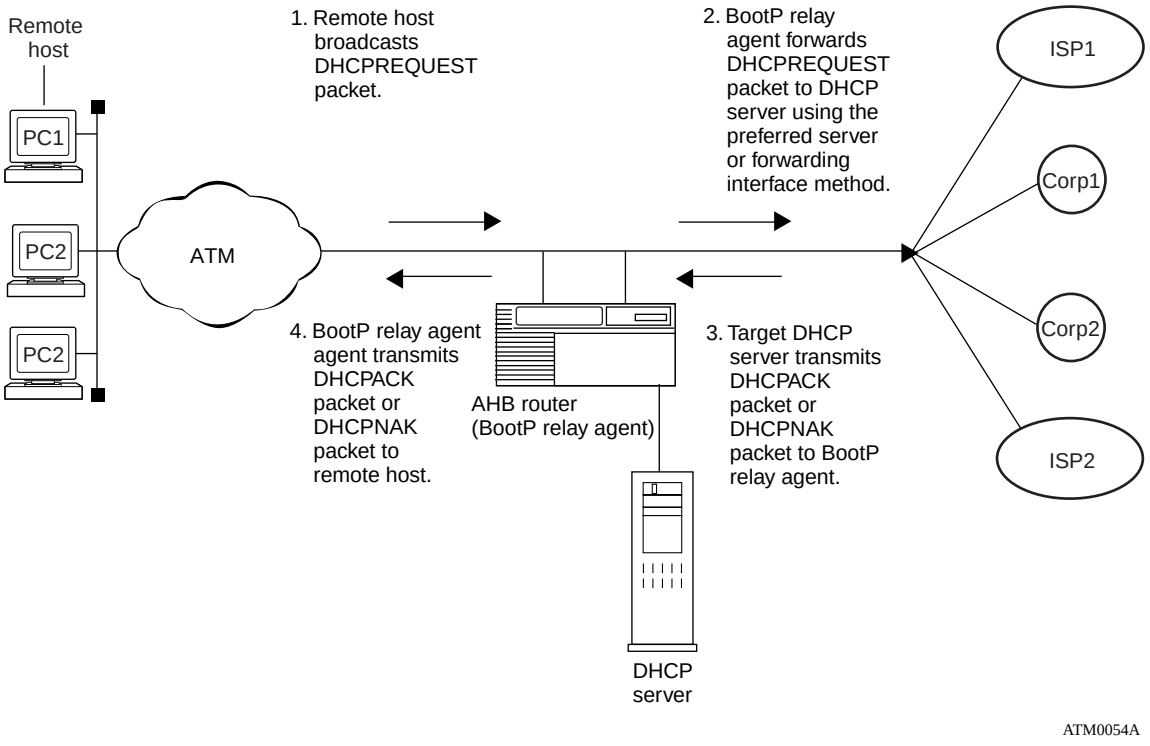

Remote host
PC1
PC2
PC2
ATM
1. Remote host broadcasts DHCPREQUEST packet.
2. BootP relay agent forwards DHCPREQUEST packet to DHCP server using the preferred server or forwarding interface method.
ISP1
Corp1
Corp2
ISP2
4. BootP relay agent agent transmits DHCPACK packet or DHCPNAK packet to remote host.
AHB router (BootP relay agent)
3. Target DHCP server transmits DHCPACK packet or DHCPNAK packet to BootP relay agent.
DHCP server
ATM0054A

Figure 1-3. How CPE Hosts Request and Receive IP Addresses from the DHCP Server

Dynamically Learning New Bridge Table Entries

The AHB router dynamically learns new bridge entries it receives from CPE hosts. You can determine the method by which AHB learns these entries by configuring the auto learning method configuration parameters on the AHB router. AHB provides the following auto learning methods:

- Unsecure
- Secure
- Both (default)
- None

Unsecure Learning Method

AHB learns new bridge entries from any IP and ARP packets it receives on ATM/AHB-configured interfaces when you set the auto learn method to unsecure or both.

Secure Learning Method

When you set the auto learning method to Secure or Both, AHB learns new bridge entries from DHCP replies sent on AHB-configured circuits. Secure entries take precedence over unsecure entries.

Before you can use secure learning mode, make sure that you:

- Configure BootP on both the unnumbered ATM interface and on the associated numbered IP interface.
- Configure a BootP preferred server or forwarding interface on the unnumbered ATM interface (use the circuit number as the IP source address).
- Verify that the IP address assigned by the DHCP server is on a different subnet than the BootP gateway address (that is, the associated numbered IP interface).

In secure learning mode, the AHB router serves as a BootP relay agent, forwarding DHCP requests it receives from CPE hosts.

When you set the learning method to both, AHB learns bridge entries either securely and unsecurely. When you set the learning method to None, AHB will not learn new bridge entries.

For information about configuring the auto learn method on an AHB router, see Chapter 3, “Setting the Auto Learn Method.”

Maintaining the AHB Bridge Table

AHB maintains a bridge table on each slot. The table contains a list of host entries to or from which the router will forward traffic. These host entries map the IP address of a CPE host to the following:

- ATM interface on which it is learned on the AHB router
- Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) number
- RFC 1483 encapsulation type
- Ethernet header information

Table 1-1 shows a sample AHB bridge table.

Table 1-1. Sample AHB Bridge Table

Host ID	Outgoing Circuit	VPI/VCI	RFC 1483 Bridge Header
200.10.10.1	2	101/31	Bridged Ethernet frame: src MAC addr= 010203040506 dest MAC adrr= 07080oaaboc Ethertype= 0800 (IP)

Adding Bridge Table Entries

In unsecure learning mode, AHB adds a new entry to the bridge table whenever it receives an IP or ARP packet that is not already in the table.

In secure learning mode, AHB adds new entries to its table when it receives certain incoming and outgoing DHCP messages. AHB adds new table entries when the CPE host on the remote site sends a DHCPDISCOVER message (source IP address equals 0.0.0.0). This new table entry identifies the incoming port, VPI/VCI, and RFC 1483 encapsulation data (including source MAC address). There is no IP address for the new table entry at this point.

AHB forwards only certain DHCP packets (ACK or NAK) to the CPE host using this entry before an IP address is assigned. When AHB receives a DHCPACK message, it updates the table entry to identify the correct IP address as provided by the DHCP server. When AHB learns the first host entry on a network, it inserts a route into the IP routing table for that network.

Removing Bridge Table Entries

AHB removes an existing table entry whenever it adds a new entry with the same source MAC address, ATM port, and VPI/VCI number. AHB also removes a table entry when it receives a DHCPRELEASE message (assuming that the source IP address-to-ATM port/VPI/VCI mapping is correct). If the entry being removed is on the original slot, all other slots that have received copies are notified to remove those entries. When AHB removes the last host entry on a network, it deletes the corresponding route from the IP routing table.

Replacing Bridge Table Entries

If the bridge table contains a bridge entry that was learned on a different circuit/PVC, and AHB learns another IP packet with the same IP address on a different circuit and VCID, then AHB replaces the old entry with the new entry. New entries that AHB learns in unsecure mode do not replace existing entries learned in secure mode, even if AHB learned them on different slots.

Using Source-Based Routing

The network provider can use source-based routing to ensure that the packet sent from a CPE host travels to the correct ISP gateway first, regardless of its destination address. The ISP gateway can be an edge router directly connected to an AHB router via a WAN interface (frame relay, PPP) or a router located within the ISP's domain. This option allows multiple links connecting the AHB router with the ISP network. If one link or edge router fails, traffic from ATM-attached hosts is routed via another edge router.

You use source-based routing by configuring an IP traffic filter on the ATM interface. You must specify traffic filter criteria and a traffic filter action. The traffic filter criteria is the range of source IP addresses allocated to CPE hosts belonging to a single ISP. You must configure a separate traffic filter for each range of source addresses that get assigned to the ATM-attached hosts by an ISP. These filters must be installed on every AHB circuit.

The traffic filter action is "forward to next hop," which identifies the ISP's gateway device. The next-hop address in the traffic filter need not be a directly attached host. If it is not a directly attached host, AHB accesses the routing table to determine the directly attached host to which the packets are sent.

You can use the “forward to next hop” feature to improve reliability. Consider an example where an ISP home network has two border routers: 200.1.2.3 and 200.3.4.5. If the source-based routing gateway address (next-hop address in the traffic filter) is advertised by both border routers, then the AHB router will send packets from the ATM-attached hosts to whichever border router has the best route. If this border router fails or if the link goes down, then the packets are sent to the alternate border router. The gateway address does not need to belong to a real device because the ISP border router forwards packets based on the destination IP address.

For information about configuring IP filters for source-based routing, see Chapter 3, “Configuring Traffic Filters for Source-Based Routing.”

Responding to Proxy ARP Requests

By default, AHB receives ARP requests from ATM-attached hosts. When the AHB router receives an ARP request, it responds to this request with its own hardware address as the target MAC address. You must enable proxy ARP separately on each circuit.

When proxy ARP is enabled, the AHB router responds to ARP requests if all of the following conditions are true:

- The ARP request received by AHB is not a self-ARP request (that is, the host IP address equals the target IP address or the source address equals 0.0.0.0).
- The host’s (sender) address is already in the bridge table or can be learned from this packet (unsecure mode enabled).
- The target host address either is in the host table and has a different circuit VPI/VCI, or the target host address is not in the bridge table.

For information about configuring proxy ARP, see Chapter 3, “Enabling and Disabling Proxy ARP on a Circuit.”

Using Inbound Packet Filtering

AHB uses inbound packet filtering to forward bridge packets it receives from CPE hosts on an AHB interface, regardless of whether an entry exists in the bridge table for that CPE host. The AHB interface must be an ATM service record with LLC/SNAP encapsulation. For information about configuring inbound packet filtering, see Chapter 3, “Enabling and Disabling Inbound Packet Filtering.”

Chapter 2
Starting AHB Services

This chapter provides instructions for starting AHB services with the default configuration values supplied by Bay Networks.

This chapter includes the following information:

Topic	Page
Network Planning Considerations	2-1
AHB Configuration Requirements	2-1
Configuring AHB Services	2-5
Configuring a DHCP/BootP Relay Agent	2-10

Network Planning Considerations

Before you configure AHB, ensure that you have the following:

- The VPI/VCI numbers (ATM) used in your network configuration
- The ATM circuit names that you configured
- A minimum of 8 MB of memory on the router for ARE processor modules

AHB Configuration Requirements

Before you can configure AHB on the router, you must:

- Prepare a configuration file.
- Configure an IP interface on the router.
- Configure circuitless IP on the router.

Preparing a Configuration File

To create a configuration file for AHB, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. Choose **Tools.**	The Tools menu opens.
2. Choose **Configuration Manager.**	The Configuration Manager window opens.
3. Choose **Local File**, **Remote File**, or **Dynamic.**	Site Manager prompts you for the configuration file you want to open.
4. Select the configuration file and click on **OK**.	The Configuration Manager window opens, displaying the router models.
5. Choose either the BLN or BCN router model and click on **Confirm**.	The Module List opens.

If you have questions about how to perform any of these preliminary tasks, refer to *Configuring and Managing Routers Using Site Manager.*

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the management information base (MIB) object ID. This process is equivalent to modifying parameters using Site Manager.

For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: Bay Networks strongly recommends that you use the Technician Interface for very minor MIB adjustments only. The Technician Interface does not validate parameter entries. Entering an invalid value can corrupt your configuration.

Proceed to the next section to configure an IP interface on the router.

Configuring an IP Interface on the Router

You must configure an IP interface on a non-ATM/AHB interface. This can be a LAN interface or a frame relay interface. You use this IP interface address as the associated IP interface when defining the unnumbered IP circuit for the AHB router.

To configure an IP interface on the router, begin at the Module List window and complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Module List, choose a **link module** (for example, Quad Ethernet).	
2. Click on a **link module connector** (for example, XCVR1).	The Add Circuit List window opens.
3. Supply a **circuit name** (or accept the default circuit name) and click on **OK**.	The Select Protocols window opens.
4. Select **IP**, then click on **OK**.	The IP Configuration window opens.
5. Specify a valid IP address in dotted-decimal notation for the **IP address** parameter (for example, 1.1.1.1). Click on **Help** or see the parameter description on page page A-15	
6. Accept the default values for the following parameters: • **Subnet Mask** • **Transmit Bcast Addr** **UnNumbered Assoc Address** Click on Help or see the parameter descriptions on page A-15.	
7. Click on **OK**.	You return to the Configuration Manager window.

Configuring Circuitless IP on the Router

To operate AHB, you must configure unnumbered IP interfaces on the router and assign an associated IP address to each interface. You can elect to use the circuitless IP address as the associated address for unnumbered interfaces.

AHB uses unnumbered interfaces because not all hosts attached via the ATM circuit are on the same IP network. Furthermore, a host may change its IP network over time (due to subscribing with different service providers), and it would be inconvenient to move the PVC for that host each time its network IP address changes.

When you configure a circuitless IP interface, note the following:

- You can configure only one circuitless IP interface per router.
- You must assign a unique IP address and subnetwork number to the circuitless IP interface.

A circuitless IP interface has an IP address that is not mapped to the address of a specific circuit. Thus, if one or more of the router's IP interfaces becomes disabled, this circuitless feature ensures that the router is always reachable using the circuitless interface address, as long as a viable path to the router exists.

For more information about circuitless interfaces, see *Configuring IP Services.*

To configure a circuitless IP interface on the router, begin at the Configuration Manager window and complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Circuitless IP**.	The Circuitless IP menu opens.
4. Choose **Create**.	The IP Configuration window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Specify a unique IP address in dotted-decimal notation for the **IP address** parameter (for example, 250.225.2.2). Click on **Help** or see the parameter description on page A-15.	
6. Specify a valid subnet mask for the **Subnet Mask** parameter (for example, 255.255.255.0). Click on Help or see the parameter description on page A-15.	
7. Click on **OK**.	Site Manager saves the circuitless IP interface, and opens a special Select Protocols window that lists the protocols that you can configure on a circuitless interface.

Go to the next section to configure AHB services on the router.

Configuring AHB Services

Configuring AHB services involves:

- Creating an ATM interface
- Adding an LLC/SNAP service record for PVCs
- Adding AHB on an LLC/SNAP service record
- Adding PVCs to the LLC/SNAP service record on an ATM interface
- Configuring a BootP relay agent

Before configuring AHB, refer to *Configuring and Managing Routers with Site Manager* for instructions about the Site Manager configuration tool and how to work with configuration files.

Creating an ATM Interface

To create an ATM interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Module List, choose an **ARE ILI link module** (for example, ARE OC-3 MM).	
2. Click on an **ATM link module connector** (labeled ATM1).	The Add Circuit window opens.
3. Supply a circuit name (or accept the default circuit name) and click on **OK**.	The Initial ATM Signaling Config window opens.
4. Change the **Enable ATM Signaling** parameter to **Disable**. Click on **Help** or see the parameter description on page A-19. You disable ATM signaling because AHB runs only on PVCs, not SVCs.	Site Manager changes the value of this parameter.
5. Click on **OK**.	The Edit ATM Connector window opens.

Go to the next section to add an LLC/SNAP service record to the ATM interface that you just created.

Adding an LLC/SNAP PVC Service Record

When you add a service record to an ATM interface, you must specify the data encapsulation type and virtual connection it uses. AHB requires that you add the LLC/SNAP data encapsulation type and the circuit (PVC) connection type for this service record.

Caution: You cannot edit the Data Encapsulation Type or Virtual Connection Type parameter once you assign it to a service record. However, you can edit the Data Encapsulation Type for individual PVCs.

For an explanation of the different data encapsulation types and rules for assigning data encapsulation, refer to *Configuring ATM Services*.

To add an LLC/SNAP service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Edit ATM Connector window, click on **Service Attributes**.	The ATM Service Records List window opens.
2. Click on **Add.**	The ATM Service Record Parameters window opens, displaying default values for the Data Encapsulation type and Virtual Connector type. Because you disabled ATM signaling when you created the circuit, the ATM Service Record Parameters window automatically changes the default for the Data Encapsulation Type parameter to Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) and the Virtual Connection Type parameter to PVC.
3. Click on **OK.**	The ATM service information appears in the ATM Service Record List and the Select Protocols window opens.

Go to the next section, "Adding AHB to the LLC/SNAP Service Record."

Adding AHB to the LLC/SNAP Service Record

When adding AHB services to an LLC/SNAP service record, remember the following:

- A PVC type service record requires that you add at least one PVC for the service record to operate.
- Each service record globally controls all protocols for any PVCs that it contains.

To add AHB to an LLC/SNAP service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, click on **AHB.**	The Configuration Manager automatically highlights IP and BootP, adding these protocols to the service record.
2. Click on **OK.**	The IP Configuration window opens, prompting you to specify IP configuration parameters.
3. Specify an unnumbered interface address (0.0.0.0) for the **IP Address** parameter. Click on **Help** or see the parameter description on page A-15.	
4. Specify the associated numbered circuit address for the **UnNumbered Assoc Address** parameter. This may be a circuitless IP interface address. Click on **Help** or see the parameter description on page A-15.	
5. Click on **OK**.	The ATM Half-Bridge Configuration window opens.
6. Accept the AHB default configuration values and click on **OK**.	The ATM Virtual Channel Link window opens.

Next, add PVCs to the LLC/SNAP service record on the ATM interface.

Adding PVCs to the LLC/SNAP PVC Service Record

To add PVCs to the LLC/SNAP service record on the ATM interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the ATM Virtual Channel Link window, click on **Add**.	The ATM Virtual Channel Link Parameters window opens.
2. Supply the following information: • A **VPI**. This number, which is part of the cell header, identifies the virtual path of the PVC. The header can contain a maximum of 8 VPI bits for a UNI connection. This bit range allows for path identifiers from 0 to 255. • A **VCI**. This number, which is part of the cell header, identifies the virtual channel of the PVC. The header can contain a maximum of 16 VCI bits. This bit range allows for channel identifiers from 0 to 65535. Click on **Help** or see the parameter descriptions on page A-23.	
3. Click on **OK**.	The ATM Virtual Channel Link window opens. For information about changing parameters in the ATM Virtual Channel Link window, refer to Appendix B.
4. To add another PVC with the default configuration, repeat steps 1 through 3.	
5. Click on **Done**.	The ATM Service Records List window opens.
6. Click on **Done**.	The Edit ATM Connector window opens.
7. Click on **Done**.	You return to the Configuration Manager window.

Note: Following the recommendation of the ATM Forum, virtual channel identifiers from 0 to 31 are reserved for signaling and added functionality.

Next, you must configure BootP to define a forwarding path between a router and a BootP/DHCP server on the network.

Configuring a DHCP/BootP Relay Agent

To allow the AHB router to successfully forward DHCP packets from CPE hosts to a DHCP server on the network, you must configure a BootP relay agent on both the unnumbered ATM/IP interface and an associated numbered interface. AHB does this automatically when you add AHB to the ATM service record. You also must define a forwarding path between the AHB router and a DHCP server on the network. You establish this forwarding path using one or both of the following methods:

- Configure one or more BootP forwarding IP interfaces on the router.

  You define one IP interface to receive DHCP request packets from the remote CPE hosts and another to transmit (broadcast) DHCP request packets to the DHCP server.

- Configure one or more BootP preferred servers on an IP interface on the AHB router.

  You define one IP interface to receive DHCP request packets from the remote CPE hosts and then unicast the requests directly to the DHCP server.

Creating a BootP Relay Agent Forwarding Interfaces

You create a BootP relay agent forwarding table for the IP interfaces that you configure to receive the incoming DHCP request packets and to forward the outgoing DHCP request packets to the DHCP server on the network. The BootP relay agent forwards DHCP request packets based on the IP addresses of the interfaces in this table. For more information about configuring a forwarding table, refer to *Configuring IP Services.*

Site Manager requires that you specify input and output addresses to configure the BootP relay agent on the AHB router. The input IP address is the ATM unnumbered interface on which the DHCP request packet is received. The ATM unnumbered interface address appears in the BootP Relay Agent table. Its last four digits are 0.0.0<*circuit_number*>, where circuit number is the unnumbered circuit that you configured.

The output IP address is the address of the local IP interface to which the DHCP packets are forwarded.

To create a BootP relay agent forwarding table, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BootP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens, displaying the IP interfaces that you configured on the AHB router (ATM PVCs, circuitless IP interface, and so forth).
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.
6. Click on **Add**.	The BOOTP Addresses window opens.
7. Add a BootP forwarding entry by setting the following parameters: • **Input IP Address** • **Output IP Address** Click on Help or see the parameter descriptions on A-11.	
8. Click on **OK**.	The BOOTP Relay Agent Forwarding Table window opens.
9. Click on **Done**.	The BOOTP Relay Agent Interface Table window opens.
10. Click on **Done**.	You return to the Configuration Manager window.

Configuring BootP Preferred Servers

You can configure a BootP preferred server by specifying the IP address of the relay agent on the router and the IP address of the target server. You configure a preferred server when you know the IP address of the DHCP server to which you want to send a DHCP request.

Specifying the Relay Agent IP Address

The relay agent IP address is the interface that you want to receive DHCP packets from a CPE host. If you configured BootP on an unnumbered interface (ATM/AHB interface), specify the associated numbered interface address for the relay agent IP address.

To specify the relay agent IP address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table opens.
6. Click on **Add**.	The BOOTP Preferred Server Configuration window opens.
7. Set the **Relay Agent IP Address** parameter. Click on **Help** or see the parameter description on page A-14.	
8. Click on **OK**.	
9. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Target Server IP Address

After you specify the relay agent IP address, you must specify the IP address of the DHCP server that should receive the DHCP packet from the BootP relay agent.

To specify the target server IP address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table opens.
6. Click on **Add**.	The BOOTP Preferred Server Configuration window opens.
7. Set the **Target IP Server** parameter. Click on **Help** or see the parameter description on page A-15.	
8. Click on **OK**.	
9. Click on **Done**.	You return to the Configuration Manager window.

Chapter 3
Customizing AHB Services

When you first configure AHB services, default values are in effect for all parameters (see parameter descriptions in Appendix A). You may want to change these values, depending on the requirements of your network.

This chapter provides information about how to customize AHB to use it effectively on your network. This chapter includes the following topics:

Topic	Page
Modifying the AHB Configuration	3-1
Modifying AHB Circuits	3-8
Configuring Traffic Filters for Source-Based Routing	3-10
Deleting AHB from the Router	3-11

Modifying the AHB Configuration

To change the way AHB operates on the router, you can modify the AHB global parameters in the Edit ATM Half-Bridge Global Parameters window (refer to Appendix A).

Enabling and Disabling AHB

By default, AHB forwards packets to and from ATM PVCs when you enable the AHB function on the router. When you disable AHB, you prevent AHB from forwarding packets to and from ATM PVCs.

To enable and disable AHB forwarding on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Global**.	The Edit ATM Half-Bridge Global Parameters window opens.
5. Set the **Enable** parameter. Click on Help or see the parameter description in Appendix A.	

Setting the Auto Learn Method

You can determine the method by which AHB automatically learns new bridge entries on the router by configuring the auto learning method. You can configure AHB in one of the following learning modes:

- Secure
- Unsecure
- Both
- None

By default, the auto learn method is set to Both. This means that AHB will learn new bridge entries either securely or unsecurely.

If you set the learning mode to Secure or Both, AHB learns new bridge entries from the DHCP reply packets sent on the AHB-configured interface. Entries learned in secure mode always take precedence over entries learned in unsecure mode.

If you set the learning mode to Unsecure or Both, AHB learns new bridge entries from IP and ARP packets received on the AHB-configured interface.

To set the auto learn method by which AHB learns bridge entries, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Global**.	The Edit ATM Half-Bridge Global Parameters window opens.
5. Set the **Auto Learn Method** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **OK.**	You return to the Configuration Manager window.

Configuring a Local AHB Init File

AHB Init files are ASCII data files that you can use to manually add bridge table entries and or configure PVCs on an AHB interface. You create the init files locally, but must store them on the router's flash memory card. AHB reads the init files from the router's flash memory when the router boots.

The AHB init files contain an extra flag on each entry that indicates where AHB should create the corresponding PVC identified in the bridge entry, if it does not already exist.

Sample Init File

In the AHB init file, there is a section for each router slot that has configured bridge entries. Slots that do not contain hosts do not need a section header. Within a section, there is one line for each bridge entry.

A sample init file (ahb.dat) is shown next:

```
[SLOT 3]

1.3.1.32 255.255.255.0 4 409600 0 0
aaaa030080c2000700001122334455 66aabbccdde eff0800

1.3.2.32 255.255.255.0 4 409600 0 0
aaaa030080c2000700007788990011 22aabbccdde eff0800

[SLOT 4]

1.4.2.32 255.255.255.0 5 409600 0 0
aaaa030080c2000700009988776655 44aabbccdde eff0800
```

The bridge entry fields (separated by spaces) are:

- Field 1 = host IP address (dotted-decimal)
- Field 2 = host subnet mask (dotted-decimal)
- Field 3 = ATM circuit number (decimal)
- Field 4 = PVC VPI/VCI (decimal, VPI in bits 0-11, VCI in bits 12-23)
- Field 5 = reference VPI/VCI (decimal)
- Field 6 = host flags (decimal, bit field)
- Field 7 = bridge header (hex, 1483 SNAP/LLC + ethernet header)

The host flag bits which can be configured are:

- Bit 0 = no protocol address, do not add bridge entry to table
- Bit 3 = add new PVC (VPI/VCI in field 4) based on reference PVC
- Bit 4 = do not forward packets that match this IP address
- Bit 7 = if set, indicates that host entry should be deleted

The bridge header has the following format:

- Octets 00-09 = encapsulate for 1483 bridged Ethernet packet
- Octets 10-15 = destination MAC address
- Octets 16-21 = source MAC address
- Octets 22-23 = protocol ID (0x800 for IP)

The reference VPI/VCI identify a preconfigured ATM PVC whose parameters are used as a template when AHB creates a new PVC.

To specify the name of the local init file you want to use, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Global**.	The Edit ATM Half-Bridge Global Parameters window opens.
5. Set the **Local Init File** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying an Alternate Init File

You can create an alternate init file (backup) as a safeguard in case the local init file fails to load properly when the router boots. You should copy the alternate init file to a different flash memory card on the AHB router.

When you boot the AHB router, it attempts to read the local init file. If the local init file is null, or if AHB cannot read the file, it then reads the alternate init file.

To specify the name of the alternate init file you want to use, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Global**.	The Edit ATM Half-Bridge Global Parameters window opens.
5. Set the **Alternate Init File** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Debug Level

You can display the level of debug messaging you want the AHB router to display in its log file by specifying a value for the Debug Level parameter.

By default, the debug level is set to 0, meaning that AHB disables all debug messages. You can specify a debug level value from 1 to 5. Specifying a higher value causes AHB to display more detailed debug messages.

To specify the debug level, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Global**.	The Edit ATM Half-Bridge Global Parameters window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Debug Level** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling and Disabling Inbound Packet Filtering

By default, inbound packet filtering is disabled on the AHB router. This means that AHB forwards bridge packets it receives from CPE hosts, regardless of whether a table entry exists in the bridge table for that host.

When you enable inbound packet filtering on the AHB router, AHB verifies that the source address in the IP packet is contained in the bridge table and that it corresponds to the circuit and virtual connection identification number (VCID) contained in the AHB bridge table. This is a check to ensure that the packets received by the AHB router are valid.

To enable and disable inbound packet filtering on the AHB router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Global**.	The Edit ATM Half-Bridge Global Parameters window opens.
5. Set the **Inbound Packet Filtering** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **OK**.	You return to the Configuration Manager window.

Modifying AHB Circuits

You can modify AHB circuits by changing the AHB circuit parameters located in the ATM Half-Bridge Circuit List window (refer to Appendix A). You may need to modify AHB circuit characteristics after you configure multiple PVCs on an ATM interface, and you have configured AHB on this interface. These parameters include:

- Enable
- Learned Host Subnet Mask
- Enabling Proxy ARP

Enabling and Disabling an AHB Circuit

You enable the bridging of packets on an AHB circuit when you configure AHB interfaces on the router. To disable the bridging of packets on AHB interfaces, set the Enable parameter to Disable.

To enable and disable the bridging of packets on an AHB circuit, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Circuit List**.	The Edit ATM Half-Bridge Circuit List window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Subnet Mask for the Learned Host

If you set the learning method on the ATM interface to Unsecure or Both, you must specify a subnet mask for a dynamically learned host. AHB uses the subnet mask to identify the host's network and to add routes to the IP routing table based on the host's IP address.

If you specify 0.0.0.0 (default) as the subnet mask for learned hosts, then AHB uses the natural class (A,B,C) subnet mask.

To specify the subnet mask for the learned host, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Circuit List**.	The Edit ATM Half-Bridge Circuit List window opens.
5. Set the **Learned Host Subnet Mask** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Enabling and Disabling Proxy ARP on a Circuit

By default, proxy ARP is enabled on the AHB circuit when you configure it. This tells the AHB router to respond to ARP requests from ATM-attached hosts with its own hardware address as the target MAC address.

You must separately enable or disable proxy ARP on each AHB circuit on the router.

To enable and disable proxy ARP on each AHB circuit, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Circuit List.**	The Edit ATM Half-Bridge Circuit List window opens.
5. Set the **Enable Proxy ARP** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Configuring Traffic Filters for Source-Based Routing

The AHB router may use source-based routing to ensure that packets sent from a CPE host travel to the correct ISP gateway first, regardless of its destination address. The ISP gateway can be an edge router directly connected to an AHB router via a WAN interface (frame relay, PPP) or a router located within the ISP domain.

You configure source-based routing by creating an IP traffic filter whose action is “forward to next hop.” You must specify the ISP gateway address (or a virtual address within the ISP domain) as the next-hop address.

For detailed information about creating traffic filters for source-based routing, refer to *Configuring Traffic Filters and Protocol Prioritization*.

Deleting AHB from the Router

To delete AHB from the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **AHB**.	The AHB menu opens.
4. Choose **Delete AHB**.	You return to the Configuration Manager window.

Appendix A
AHB, BootP/DHCP, IP, and ATM Parameter Descriptions

This appendix contains reference information about customizing AHB global configuration and AHB circuit parameters. It also contains a subset of parameter descriptions for BootP/DHCP, IP, and ATM that you can use to configure AHB.

Topic	Page
AHB Global Parameters	A-2
AHB Circuit Parameters	A-6
BootP Relay Agent Interface Table Parameters	A-8
BootP Address Parameters	A-10
BootP Relay Agent Preferred Server Table Parameters	A-12
BootP Preferred Server Configuration Parameters	A-14
IP Configuration Parameters	A-15
ATM Interface Parameter Descriptions	A-17
ATM Service Record Parameter Descriptions	A-19
ATM Virtual Channel Link Parameter Descriptions	A-23

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function

- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

AHB Global Parameters

Use the following guidelines to configure AHB global parameters in the Edit ATM Half-Bridge Global Parameters window (Figure A-1). The Edit ATM Half-Bridge Global Parameters window contains parameters that allow you to customize AHB operation.

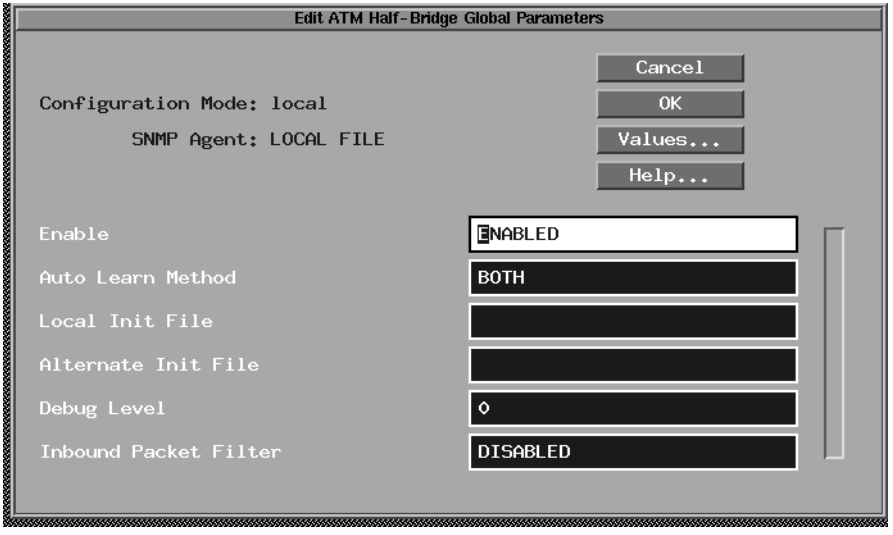


Figure A-1. Edit ATM Half-Bridge Global Parameters Window

The AHB global parameter descriptions follow.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > AHB > Global

Default: Enabled

Options: Enable | Disabled

Function: Enables or disables AHB packet forwarding to and from ATM PVCs.

Instructions: Select Disable to disable AHB on this interface without deleting it. Select Enable to reenable AHB services if you previously disabled it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.1 #2

Parameter: Auto Learn Method

Path: Configuration Manager > Protocols > IP > AHB > Global

Default: None

Options: Secure | Unsecure | Both | None

Function: Specifies the method by which AHB dynamically learns new bridge entries on the router.

Instructions: By default, the auto learn method is set to Both. This means that AHB will learn new bridge entries either securely or unsecurely.

If you set the learning mode to Secure or Both, AHB learns new bridge entries from the DHCP reply packets sent on the AHB-configured interface. Entries learned in secure mode always take precedence over entries learned in unsecure mode.

If you set the learning mode to Unsecure or Both, AHB learns new bridge entries from IP and ARP packets received on the AHB-configured interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.1 #3

Parameter: Local Init File

Path: Configuration Manager > Protocols > IP > AHB > Global
Default: None
Options: None
Function: Specifies a local ASCII data file into which you can add bridge table entries for configuring PVCs on an AHB interface. You create init files locally, but you must store them on the router's flash memory card. AHB loads the init files when the router boots.
Instructions: Specify the name of the init file you want to use. Be sure to copy the file to the router's flash memory so the router can boot with this file.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.1 #4

Parameter: Alternate Init File

Path: Configuration Manager > Protocols > IP > AHB > Global
Default: None
Options: None
Function: Specifies an alternate init file (backup) as a safeguard in case the local init file fails to load properly when the router boots.
Instructions: Specify the alternate init file name.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.1 #5

Parameter: Debug Level

Path: Configuration Manager > Protocols > IP > AHB > Global
Default: 0
Options: Recommended values are from 1 to 5
Function: Specifies the level of debug messaging you want to display in the log file for AHB.
Instructions: Enter the debug messaging level you want.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.1 #6

Parameter: Inbound Packet Filtering

Path: Configuration Manager > Protocols > IP > AHB > Global

Default: Disabled

Options: Enabled │ Disabled

Function: By default, inbound packet filtering is disabled on the AHB router. This means that AHB forwards bridge packets it receives from CPE hosts, regardless of whether a table entry exists in the bridge table for that host.

When you enable inbound packet filtering on the AHB router, AHB verifies that the source address in the IP packet is contained in the bridge table and that it corresponds to the circuit and virtual connection identification number (VCID) contained in the AHB bridge table. This is a check to ensure that the packets received by the AHB router are valid.

Instructions: Choose Enable to enable packet filtering on the AHB router. Choose Disable to disable packet filtering on the AHB router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.1 #7

AHB Circuit Parameters

Use the following guidelines to configure AHB Circuit parameters in the ATM Half-Bridge Circuit List window (Figure A-2).

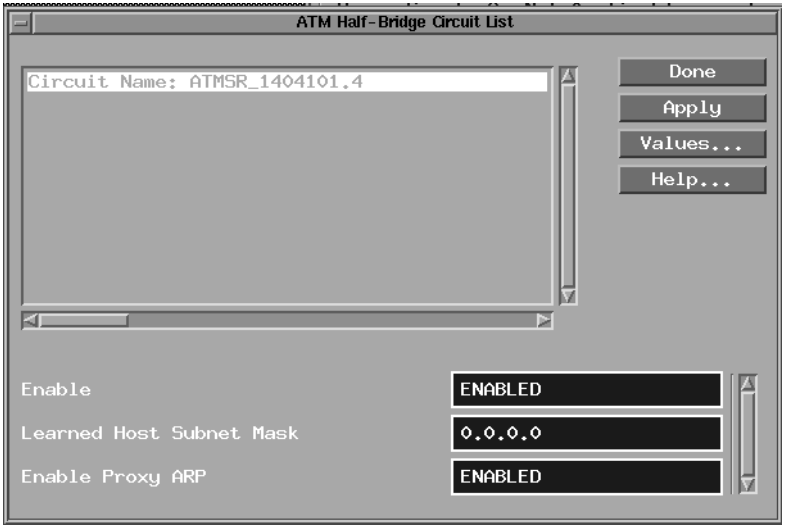


Figure A-2. ATM Half-Bridge Circuit List

The AHB circuit list parameters follow.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > AHB > Circuit List

Default: Enabled

Options: Enabled | Disabled

Function: Enables or disables AHB packet forwarding to and from CPE hosts connected via this circuit.

Instructions: Choose Enable to enable AHB packet forwarding on this circuit. Choose Disable to disable packet forwarding on this AHB circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.2.1 #2

Parameter: Learned Host Subnet Mask

Path: Configuration Manager > Protocols > IP > AHB > Circuit List

Default: 0.0.0.0

Options: None

Function: Applies only when you set the auto learning method to Unsecure or Both. When you specify a subnet mask for the learned host, AHB uses this subnet mask specified in the MIB entry wfAhbCircuitEntry.afAhbCctDefSubNetmask<cct>, where <*cct*> represents the circuit on which the host is learned.

Instructions: Specify a valid subnet mask for the learned host. If you specify 0.0.0.0 (default), then AHB uses the natural class (A,B,C) subnet mask.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.2.1 #4

Parameter: Enable Proxy ARP

Path: Configuration Manager > Protocols > IP > AHB > Circuit List

Default: Enable

Options: Enabled | Disabled

Function: Specifies whether or not the AHB router responds to ARP requests sent from ATM-attached hosts on the remote network.

Instructions: Choose Enable to allows AHB to respond to ARP requests from ATM-attached hosts. Choose Disable to prevent AHB from responding to ARP requests from AHB-attached hosts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.13.2.1 #5

BootP Relay Agent Interface Table Parameters

Use the following guidelines to configure DHCP parameters in the BOOTP Relay Agent Interface Table window (Figure A-3). This table lists all the IP interfaces that you configured on the AHB router. It contains parameters that allow you to change the way the BootP relay agent operates.

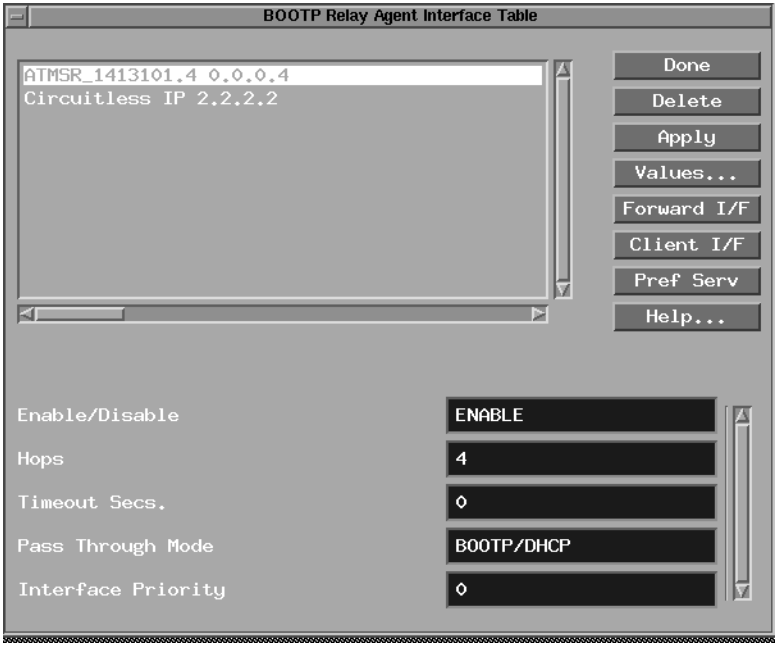


Figure A-3. BOOTP Relay Agent Interface Table Window

The BOOTP relay agent interface table window parameter descriptions follow.

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: Enable

Options: Enable | Disable

Function: Specifies whether BootP is active on the network interface.

Instructions: Select Enable to enable BootP on the network interface; select Disable to disable BootP on the network interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.2

Parameter: Hops

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 4

Options: 1 to 16 hops

Function: Specifies the maximum number of hops from the CPE host to the DHCP server. A hop is the logical distance between two devices. If the value in the hops field of a DHCP packet is greater than the number you specify for this parameter, the router drops the packet.

Instructions: Accept the default of 4 hops or specify a number from 1 to 16.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.5

Parameter: Timeout Secs.

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 0

Options: 0 to 65535 seconds

Function: Specifies the minimum number of seconds that the router waits before forwarding a DHCP packet. If the value in the seconds field of a DHCP packet is less than the value you specify for this parameter, the router drops the packet.

Instructions: Accept the default, 0, or specify a number from 1 to 65535.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.6

Parameter:	**Pass Through Mode**
Path:	Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table
Default:	BOOTP
Options:	BOOTP | DHCP | BOOTP and DHCP
Function:	Specifies whether the interface relays BootP, DHCP, or both BootP and DHCP requests.
Instructions:	Select BOOTP to relay BootP requests; select DHCP to relay DHCP requests; select BOOTP and DHCP to relay both kinds of requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.1.1.16

BootP Address Parameters

Use the following guidelines to configure DHCP parameters in the BOOTP Addresses window. The BOOTP Addresses window (Figure A-4) contains parameters that allow you to specify the IP interface addresses (input/output) that you want to receive and forward DHCP packets.

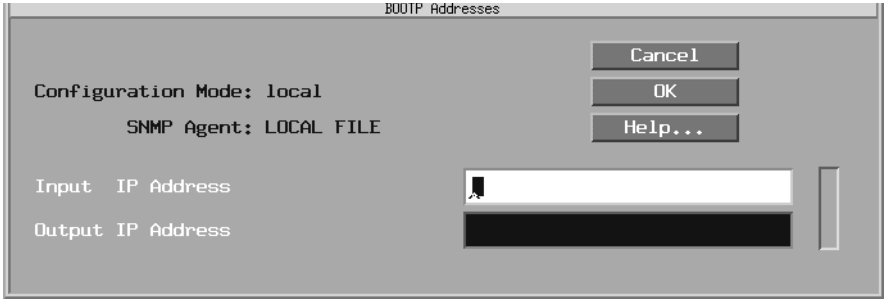


Figure A-4. BOOTP Addresses Window

To access the BOOTP Addresses window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists the IP interfaces that you configured on the router.
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.
6. Click on **Add**.	The BOOTP Addresses window opens.

The BootP address parameter descriptions follow.

Parameter: Input IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that receives DHCP packets from CPE hosts.

Instructions: Enter the IP address of an interface that you want to receive DHCP packets from CPE hosts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.3

Parameter: **Output IP Address**

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that forwards DHCP packets to an external network.

Instructions: Enter the IP address of a numbered network interface that you want to send DHCP packets to CPE hosts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.4

BootP Relay Agent Preferred Server Table Parameters

Use the following guidelines to configure BootP preferred server parameters in the BOOTP Relay Agent Preferred Server Table window (Figure A-5). This table contains parameters that allow you to customize BootP relay agent preferred server functions.

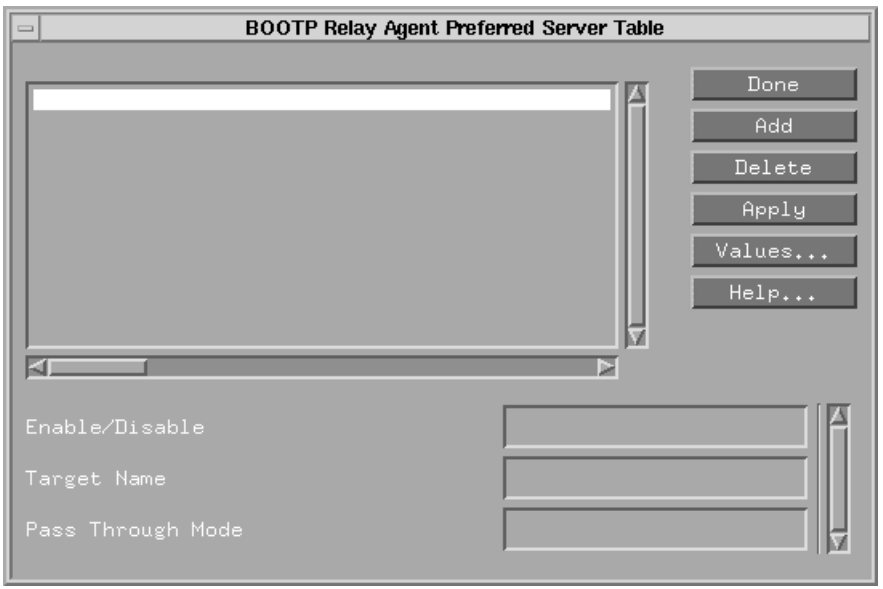


Figure A-5. BOOTP Relay Agent Preferred Server Table Window

The BootP relay agent preferred server parameters descriptions follow:

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: Enable

Options: Enable | Disable

Function: Specifies whether the forwarding route is active.

Instructions: Select Enable to allow DHCP forwarding through this route; select Disable to prevent DHCP forwarding through this route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.2

Parameter: Target Name

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces

Function: Specifies the target server's host name.

Instructions: To keep track of the names of DHCP servers, enter the target server's host name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.5

Parameter: Pass Through Mode

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: BOOTP

Options: BOOTP | DHCP | BOOTP and DHCP

Function: Specifies whether the interface relays BootP, DHCP, or both BootP and DHCP requests.

Instructions: Select BOOTP to relay BootP requests; select DHCP to relay DHCP requests; select BOOTP and DHCP to relay both kinds of requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.6

BootP Preferred Server Configuration Parameters

The BOOTP Preferred Server Configuration window (Figure A-6) contains parameters that allow you to specify the IP address of the relay agent on the router and the IP address of the target server.

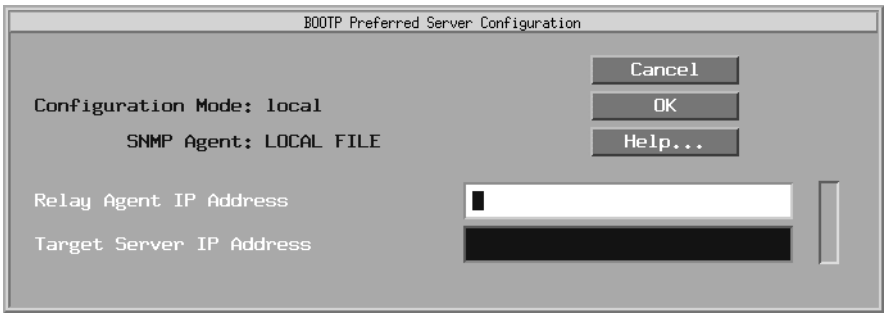


Figure A-6. BOOTP Preferred Server Configuration Window

The BootP preferred server configuration parameter descriptions follow.

Parameter: Relay Agent IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that receives DHCP packets from CPE hosts.

Instructions: Enter the IP address of a numbered network interface that you want to receive DHCP packets from CPE hosts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.3

Parameter: **Target Server IP Address**

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the address of the DHCP server that should receive DHCP packets.

Instructions: Enter the IP address of the DHCP server that should receive DHCP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.4

IP Configuration Parameters

Parameter: **IP Address**

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: 0.0.0.0 or any valid IP address

Function: Assigns a 32-bit IP address to the interface.

Instructions: Enter the IP address of the interface in dotted-decimal notation. Enter 0.0.0.0 to configure an unnumbered interface on the circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.4

Parameter: **Subnet Mask**

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: The Configuration Manager automatically calculates an appropriate subnet mask, depending on the class of the network to which the interface connects. However, you can change the subnet mask with this parameter.

Function: Specifies the network and subnetwork portion of the 32-bit IP address.

Instructions: Either accept the assigned subnet mask or enter another subnet mask in dotted-decimal notation. Enter 0.0.0.0 if you are configuring an unnumbered interface on the circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.6

Parameter: Transmit Bcast Addr

Path: Select IP from the Select Protocols window and click on OK.

Default: 0.0.0.0

Options: 0.0.0.0 or any valid IP broadcast address

Function: Specifies the broadcast address that this IP subnet uses to broadcast packets. Accepting 0.0.0.0 for this parameter specifies that the IP router will use a broadcast address with a host portion of all 1s. Accepting 0.0.0.0 does not configure the router to use the address 0.0.0.0 to broadcast packets. For example, if you have IP address 123.1.1.1 and a subnet mask of 255.255.255.0, accepting the default value 0.0.0.0 configures the IP router to use the address 123.1.1.255 to broadcast packets. To set the explicit broadcast address of all 1s, enter 255.255.255.255 for this parameter.

Instructions: Accept the default, 0.0.0.0, unless the calculated broadcast address (host portion) of all 1s is not adequate. If this is the case, then enter the appropriate IP broadcast address in dotted-decimal notation. If you set the IP Address parameter to 0.0.0.0 (to configure an unnumbered interface), Site Manager automatically sets this parameter to 255.255.255.255.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.8

Parameter: UnNumbered Assoc Address

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: Any valid IP address

Function: Specifies an address that IP uses when sourcing a packet. RIP uses this address to make decisions about advertising subnets over the unnumbered interface. RIP advertises subnets over the unnumbered interface if the subnets have the same mask as the associated address.

Instructions: Specify the address of any numbered interface on the router. If you are running RIP over the unnumbered interface and if you are using a subnet address as the associated address, the local and remote associated addresses should have the same network number. If you configure local and remote associated addresses using different network numbers, you must use RIP2 mode.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.110

ATM Interface Parameter Descriptions

Interface parameters define the state of the ATM interface. Figure A-7 shows the window sequence for the interface attributes category.

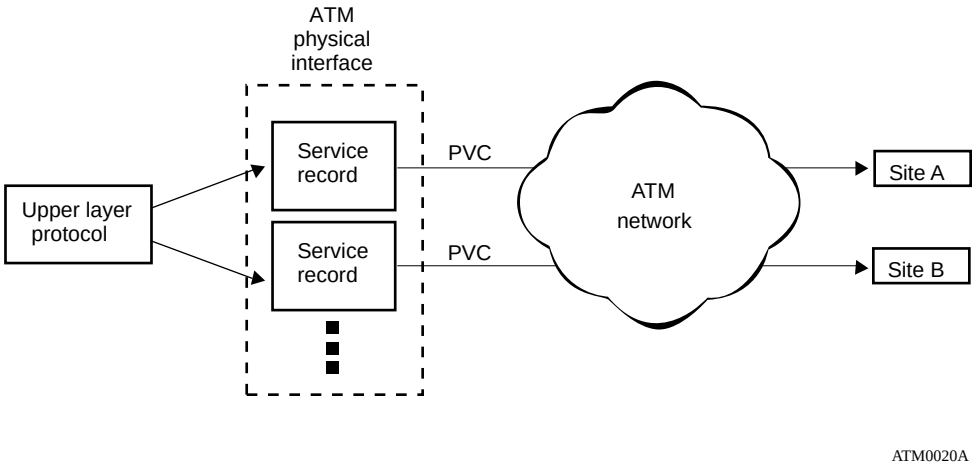


Figure A-7. Interface Attributes Window Sequence

Parameter: Administrative State

Path: Configuration Manager > Protocols > ATM > Interfaces

Default: Up

Options: Up │ Down

Function: Specifies whether this interface is enabled or disabled.

Instructions: Accept the default, Up, if you want traffic to flow over this interface. Set the state to Down if you do not want traffic to flow over this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.1.1.3

Parameter:	**Use Hardware MAC Address**
Path:	Configuration Manager > Protocols > ATM > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether or not to use the hardware MAC address for this interface. When this parameter is enabled, the Configuration Manager uses the ATM hardware MAC address of the link module for the end station identifier when automatically generating the user part (suffix) of an SVC service record ATM address. When this parameter is disabled, the Configuration Manager uses the value specified in the MAC Address Override parameter to define the end station identifier when automatically generating the user part (suffix) of an SVC service record ATM address.
Instructions:	Accept the default, Enable, if you want to use the MAC address of the ATM interface when automatically generating the end station identifier portion of the ATM address user part. Set this parameter to Disable if you want to use the MAC Address Override value when automatically generating the end station identifier portion of the ATM address user part. If you set this parameter to Disable, you must enter a value for the MAC Address Override parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.1.1.1.18

Parameter: Enable ATM Signaling

Path: Configuration Manager > Protocols > ATM > Interfaces

Default: Enable

Options: Enable │ Disable

Function: Specifies whether ATM signaling is enabled or disabled for this interface.

Signaling allows you to configure switched features (for example, SVCs and LANE) on the interface.

If you do not intend to configure any switched features on this interface (that is, you want this interface to run only PVCs), disabling this parameter makes additional system resources available.

Instructions: Accept the default, Enable, if you want to enable signaling on this interface. Set the state to Disable if you want to disable signaling on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.1.1.16

ATM Service Record Parameter Descriptions

Service record parameters define the ATM service records for an interface. The ATM Service Records List window also provides access to:

- Specific PVC parameters (PVC service records only)
- All SVCs on that service record (SVC service records only)
- LEC attributes (SVC service records using LANE data encapsulation)

Figure A-8 shows the sequence of windows that can appear when you select the service attributes category and configure a PVC.

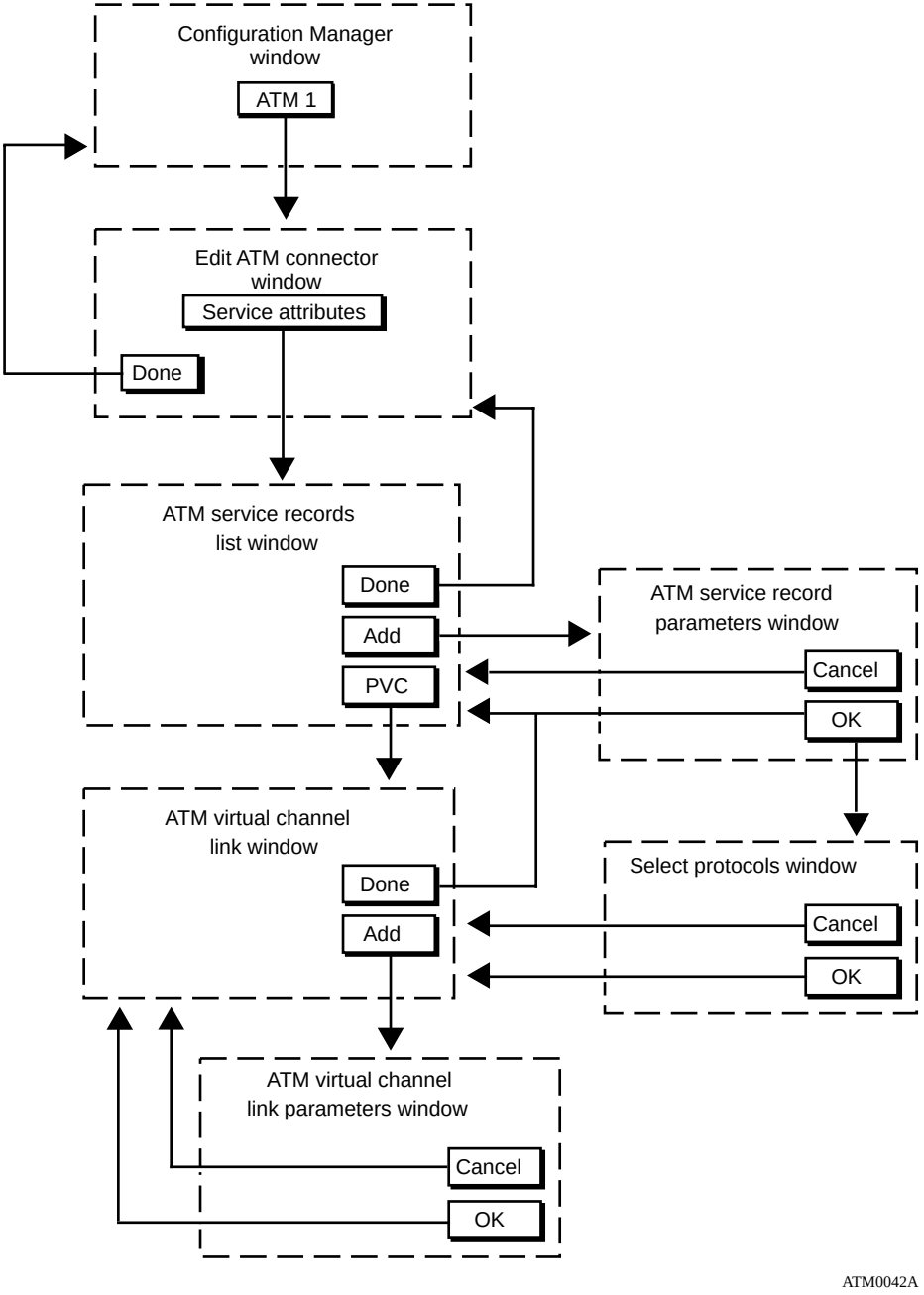


Figure A-8. Service Attributes Window Sequence (PVCs)

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > ATM > Service Records

Default: Enable

Options: Enable | Disable

Function: Enables or disables this service record.

Instructions: Accept the default, Enable, if you want traffic to flow on this service record and its VCs. Set to Disable if you do not want traffic to flow on this service record or any of its VCs.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.2.1.2

Parameter: Data Encapsulation Type

Path: Configuration Manager > Protocols > ATM > Service Records > **Add**

Default: LANE (signaling enabled) or LLC/SNAP (signaling disabled)

Options: LANE | LLC/SNAP | NLPID | NULL

Function: Identifies the data encapsulation type for this service record.

You can use this parameter to select:

- LLC/SNAP, NLPID, or NULL data encapsulation for service records containing PVCs
- LLC/SNAP data encapsulation for service records containing hybrid PVCs
- LANE for service records containing SVCs over which you want to run LAN emulation
- LLC/SNAP or NULL for service records containing SVCs over which you want to run classical IP (RFC 1577)

If you select NULL, the router interprets this as virtual, channel-based multiplexing, which is not supported for bridging.

Instructions: Select a data encapsulation type.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.2.1.5

Parameter: **ATM Addr User Part**

Path: Configuration Manager > Protocols > ATM > Service Records > **Add**

and

Configuration Manager > Protocols > ATM > Service Records

Default: None

Options: 00000000000000 to FEFFFFFFFFFFF

Function: The Configuration Manager allows you to autogenerate this parameter (see the User Part Autogeneration parameter in *Configuring ATM Services*). Depending on the settings in the ATM Interface Attributes window, this parameter can autogenerate this address using:

- The 6-byte hardware MAC address of the ATM interface
- A MAC Address Override value that you specify

In both cases, autogeneration creates a unique selector byte for each service record on the interface.

Instructions: Enter a value in the range specified.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.2.1.9

ATM Virtual Channel Link Parameter Descriptions

Note: ATM does not allow duplicate VPI/VCI pairs on the same physical interface. However, duplicate VPI/VCI pairs can exist on different physical interfaces.

Parameter: VPI Number

Path: Configuration Manager > Protocols > ATM > Service Records > **PVC** > **Add**

Default: None

Options: 0 to 255

Function: Identifies the virtual path of the PVC. The VPI is part of the cell header. The header can contain a maximum of 8 VPI bits for a UNI connection. This bit range allows for path identifiers from 0 to 255.

Instructions: Enter a value from 0 to 255.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.5.1.3

Note: Following the recommendation of the ATM Forum, virtual channel identifiers from 0 to 31 are reserved for signaling and added functionality.

Parameter: **VCI Number**

Path: Configuration Manager > Protocols > ATM > Service Records > **PVC** > **Add**

Default: None

Options: 32 to 65535

Function: Identifies the virtual channel of the PVC. The VCI is part of the cell header. The header can contain a maximum of 16 VCI bits. This bit range allows for path identifiers from 0 to 65535.

Instructions: Enter a value from 32 to 65535.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.5.1.4

Note: Following the recommendation of the ATM Forum, virtual channel identifiers from 0 to 31 are reserved for signaling and added functionality.

Parameter: **Hybrid/Bridged VC**

Path: Configuration Manager > Protocols > ATM > Service Records > **PVC**

Default: No

Options: Yes | No

Function: Specifies whether the VC is set to hybrid access mode.

Instructions: Accept the default, No, if you want the VC to work in group access mode only. Set to Yes if you want the VC to operate as a hybrid VC.

For more information about the group and hybrid access modes, see *Configuring ATM Services*.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.5.1.25

Appendix B
Understanding ATM Concepts

This appendix provides an overview of basic ATM concepts and the specific ways Bay Networks implements these concepts on BayRS routers. You must understand basic ATM concepts and terminology before you can begin using ATM Half-Bridge services.

ATM General Information

Before you can begin using ATM Half-Bridge services, you must understand some basic ATM concepts and how ATM works.

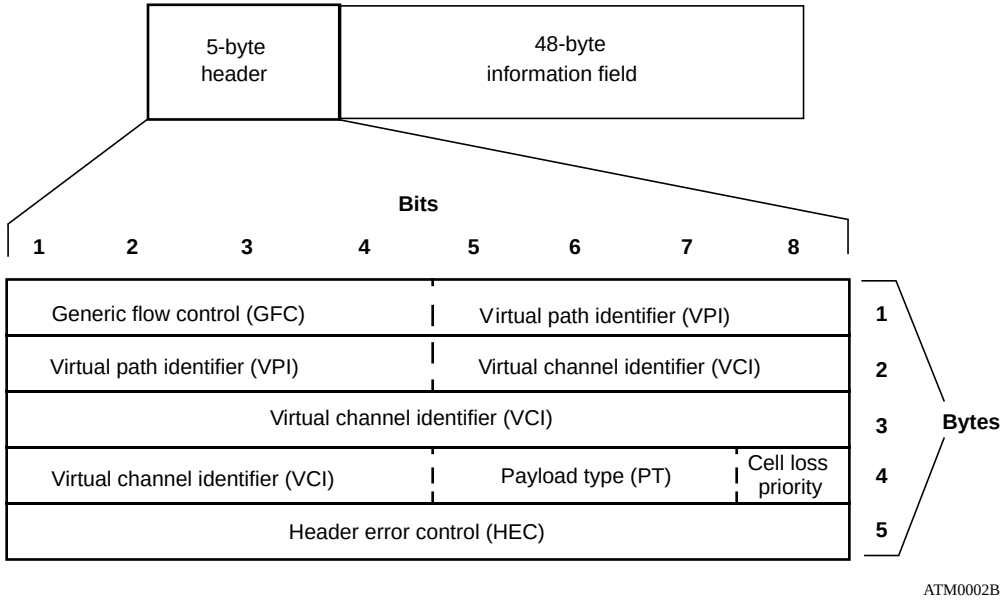
Asynchronous Transfer Mode (ATM) is a connection-oriented, cell-based technology that relays traffic across a Broadband Integrated Services Digital Network (B-ISDN). It is a cost-effective way of transmitting voice, video, and data across a network.

ATM Cells

An ATM cell is a short, fixed-length packet of 53 bytes. It consists of a 5-byte header containing address information and a fixed, 48-byte information field. Figure B-1 shows a diagram of an ATM cell.

Cell Headers

After dividing the data into 48-byte segments for transmission, the end device (that is, the ATM DSU/CSU or native ATM device) attaches the required header information (Figure B-1).



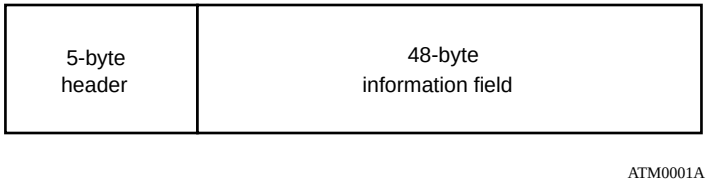


Figure B-1. ATM Cell

The fields in each ATM cell header provide all the information necessary for networking. These fields include the following:

- **Generic Flow Control (GFC)**: The first 4 bits of the cell header contain the GFC. The GFC controls traffic flow onto the ATM network by controlling the user-network interface (UNI).
- **Virtual Path Identifier (VPI)**: The next 8 bits of the cell header (that is, the last half of byte 1 and the first half of byte 2) contain the VPI. The VPI specifies a virtual path on the physical ATM link. See the next section, "ATM Data Transmission," for additional information on virtual paths.
- **Virtual Channel Identifier (VCI)**: The next 16 bits of the cell header (that is, the last half of byte 2, all of byte 3, and the first half of byte 4) contain the VCI. The VCI specifies a virtual channel within the virtual path on the physical ATM link. See the next section, "ATM Data Transmission," for additional information on virtual channels.
- **Payload Type (PT)**: The next 3 bits (that is, bits 5 to 7 of byte 4) indicate the type of information the cell is carrying (for example, user data or management information).
- **Cell Loss Priority (CLP)**: The last bit of byte 4 indicates the priority of the cell and whether the network can discard it under heavy traffic conditions. Setting the bit to 1 indicates that the network may discard the cell if necessary.
- **Header Error Control (HEC)**: The last byte of the header field contains the HEC. Its primary function is to guard against misdelivery of cells due to header or single bit errors. However, the HEC does not gauge the quality of the data in the information field.

ATM Data Transmission

Data transmission (also called *cell switching*) through the ATM network relies on the establishment of logical connections between ATM entities. ATM is a *connection-oriented* service. This means that an ATM entity cannot transmit information until it establishes a connection with a receiving entity. These connections consist of *virtual channels*, *virtual paths*, and *transmission paths*.

A virtual channel is a logical connection between two communicating ATM entities. Each virtual channel may carry a different protocol or traffic type. The virtual channel transports cells that have a common identifier. The identifier is called the virtual channel identifier (VCI) and is part of the cell header. You can establish virtual channels permanently or set them up dynamically, allowing the network to adjust itself to the traffic demand.

A virtual path is a set of virtual channels between a common source and destination. The virtual channels in a virtual path logically associate with a common identifier. This identifier is called the virtual path identifier (VPI) and is part of the cell header. You can base cell switching on either the VPI alone or on a combination of the VPI and VCI.

Virtual paths enable you to separate network transport functions into those related to an individual logical connection (virtual channel) and those related to a group of logical connections (virtual path).

A transmission path is a physical connection that comprises several virtual paths, each virtual path containing several virtual channels. The transmission path may support multiple virtual paths across a single connection to the network.

Figure B-2 shows the relationships between the virtual channel, the virtual path, and the transmission path.

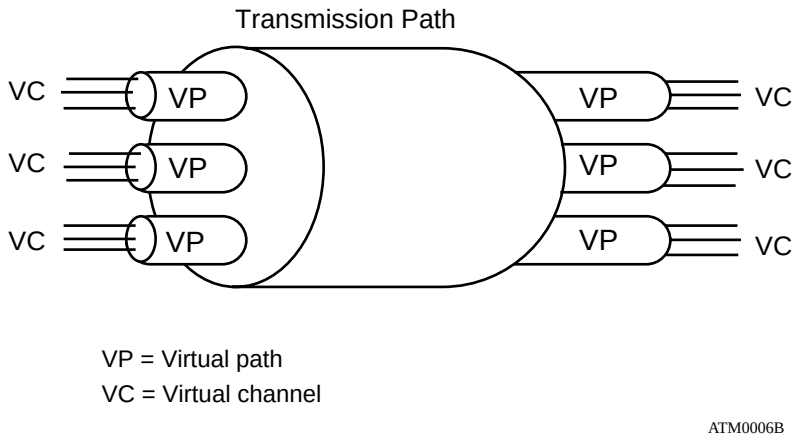


Figure B-2. ATM Transmission Components

Permanent Virtual Connections

Virtual channels and virtual paths allow you to establish virtual channel links (VCLs). To use the ATM Half-Bridge protocol, you must create VCLs as permanent virtual circuits (PVCs). Once you establish a PVC, you can transfer information over it at any time.

Service Records and Virtual Circuits

ATM devices communicate using virtual circuits (VCs). These VCs transmit and receive ATM cells containing upper-layer protocols. Bay Networks ATM routers use service records to provide a way of creating logical interfaces (within the physical ATM interface) for these upper-layer protocols. In essence, these service records allow you to:

- Organize multiple VCs into logical groups.
- Create direct, point-to-point connections.
- Assign, delete, and modify upper-layer protocols for just one PVC, or for a group of VCs, at any given time.

Data Encapsulation

Bay Networks ATM routers support multiprotocol encapsulation (as defined in RFC 1483), enabling the router to multiplex (combine) and demultiplex (separate) bridged or routed protocol data units (PDUs).

For transmission, the encapsulation process adds a header between 2 and 8 octets in length to the PDU to allow decoding. The decoding process determines the proper service access point (SAP).

When receiving information, the encapsulation method evaluates the header to determine whether the PDU is a valid routed or bridged cell. If it is valid, the encapsulation method then strips the header from the cell and passes it to the appropriate SAP for routing or bridging.

Assigning a Data Encapsulation Type for a PVC

With AHB, you must assign the Logical Link Control/Subnetwork Access Protocol (LLC/SNAP; RFC 1294) to the PVC that you create. LLC/SNAP encapsulation attaches an LLC/SNAP header before the PDU. This header includes information that the receiver needs to properly process the incoming PDU.

When assigning a data encapsulation type to a PVC or group of PVCs, keep the following in mind:

- The Site Manager ATM Service Records List and ATM Virtual Channel Link windows initially contain a default data encapsulation type of LLC/SNAP.
- When you add a PVC, it reads and uses the data encapsulation type specified in its ATM service record.
- You can globally assign a data encapsulation type to all nonhybrid PVCs in a particular service record, or you can assign a data encapsulation type to individual group PVCs using the Site Manager ATM Virtual Channel Link window.

Caution: Changing the data encapsulation type at the service record level changes the data encapsulation type for all nonhybrid PVCs on that service record. For example, if you change the ATM service record data encapsulation type from LLC/SNAP to NULL, the data encapsulation type for all PVCs (except hybrid PVCs) on that service record changes to NULL. Site Manager does not ask you to verify this change.

- If you change the data encapsulation value in the Site Manager ATM Service Records List window, all new PVCs that you add to that service record use the new value.

PVC Access Methods

For AHB, you can set up PVCs to access an ATM network in the following ways:

- Multiple PVCs per sevice record
- One PVC per service record

Multiple PVCs

Of the two methods, having multiple PVCs per service record uses network addressing most efficiently and is the easiest to configure.

Upper-layer protocols treat each service record on an ATM network interface as a single access point. These protocols use a single network address to send all traffic destined for the network to the ATM network interface. Figure B-3 shows a conceptual drawing of multiple PVCs accessing an ATM network through one service record.

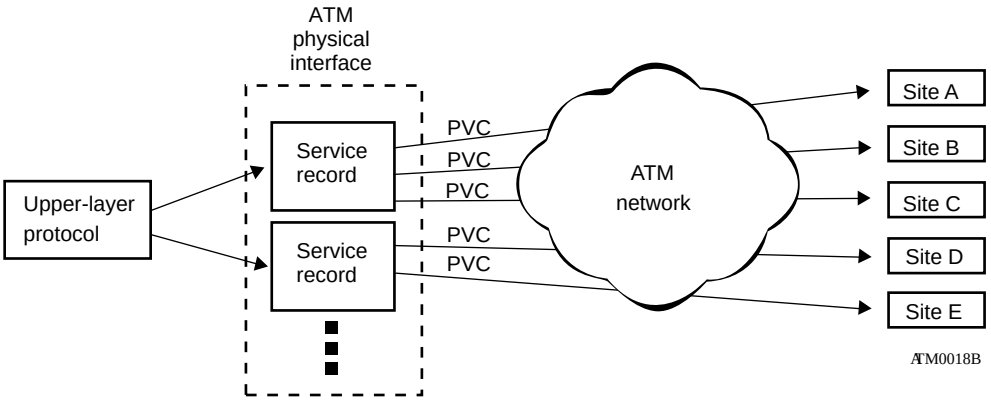


Figure B-3. Multiple PVCs per Service Record

Although you need to configure each PVC manually, you need only define and associate protocols with the ATM network service record. All the PVCs that you configure for a given ATM service record carry the protocols that you select and configure to run on that service record.

Note: When you configure multiple PVCs per service record, the PVCs all use the data encapsulation type that you set for the ATM service record (that is, the value of the Data Encapsulation Type parameter set in the ATM Service Records List window). Refer to “Data Encapsulation,” earlier in this chapter, for more information.

Multiple PVCs per service record work best in either fully meshed environments or in nonmeshed environments where systems not directly connected to each other have no need to communicate. You can configure multiple PVCs per service record as long as you do not need to separate protocols by PVC (that is, all PVCs accept the same protocols).

There are, however, ways to configure upper-layer protocols, such as IP or Internet Packet Exchange (IPX), to allow systems in nonmeshed networks to fully communicate. See the documentation for these upper-layer protocols for more information.

One PVC

One PVC per service record works the same way as multiple PVCs per service record, except that you assign only one PVC per service record.

This type of configuration is best suited to small, nonmeshed configurations, or to configurations in which protocols must reside on separate PVCs. When you define only one PVC per service record, upper-layer protocols treat the ATM network as a series of direct, point-to-point connections, viewing each PVC as an individual network interface.

You can, therefore, configure each PVC with different protocols and parameter settings. This allows you to connect to different network sites using, for example, different types of data encapsulation (Figure B-4).

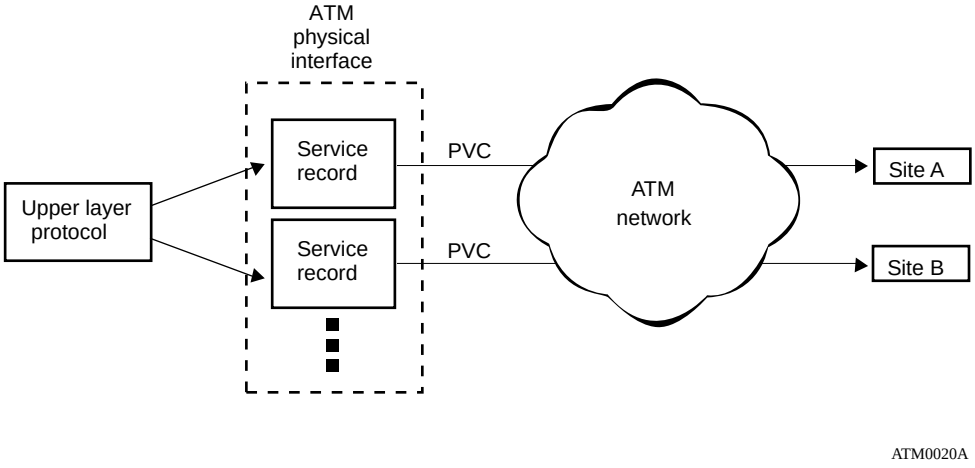


Figure B-4. One PVC per Service Record

Assigning one PVC per service record allows you to dedicate a PVC to a particular protocol, but at the expense of some configuration overhead, memory, and address space.

Note: The maximum number of PVCs you can configure in this way varies, depending on the configuration of the router, the number of protocols running on the circuits, and the number of routing entries.

Index

A

adding
- ATM circuit, 2-6
- ATM to the router, 2-9
- PVCs, 2-9
- service records
  - PVC, 2-7

Administrative State
- parameter description, A-17

ADSL terminal unit, central devices (ATU-C), 1-2

ADSL terminal unit, remote end devices (ATU-R), 1-2

Alternate Init File parameter, 3-5, A-4

ARP requests, 1-9

ATM, 1-3
- cell
  - described, B-1
  - switching, B-3
  - technology, B-1
- circuit, adding, 2-6
- concepts, B-1 to B-5
- data transmission, B-3
- transmission path, defined, B-4
- virtual channel, defined, B-4
- virtual path, defined, B-4

ATM Addr User Part
- parameter description, A-22

ATM Half-Bridge (AHB)
- auto learning methods
  - both, 1-3
  - none, 1-3
  - secure, 1-3
  - unsecure, 1-3
- bridge entries
  - adding, 1-9
  - deleting, 1-9
  - removing, 1-9
- concepts and terminology, 1-1
- configuration, 2-5
- configuration requirements, 2-1
- described, 1-1
- forwarding inbound packets, 1-4
- maintaining the bridge table for, 1-3
- modifying the AHB configuration, 3-1
- network planning considerations, 2-1
- responding to ARP requests, 1-9
- starting, 2-1
- using inbound packet filtering, 1-12
- using source-based routing, 1-9

Auto Learn Method parameter, 3-2, A-3

B

BootP
- configuring preferred servers, 2-12
- defining forwarding paths, 2-10

Broadband Integrated Services Digital Network (B-ISDN), B-1

C

cell
- switching, B-3
- technology, B-1

circuitless IP interface
- configuring, 2-4

Configuration, A-6, A-19, A-22

customer support
- programs, xvii
- Technical Solutions Centers, xvii

D

Data Encapsulation Type
  parameter description
    service record, A-21
Debug Level parameter, 3-6, A-4
DHCP
  defining forwarding paths, 2-10
  using to dynamically assign IP addresses, 1-3
digital subscriber line (DSL), 1-1
DSL access multiplexor (DSLAM), 1-2

E

Enable ATM Signaling
  parameter description, A-19
Enable parameter, A-3, A-6
Enable Proxy ARP parameter, 3-10, A-7
Enable/Disable (service record)
  parameter description, A-21
encapsulation, multiprotocol, B-5

F

forwarding paths, BootP and DHCP, 2-10

H

Hops parameter, A-9
Hybrid/Bridged VC
  parameter description, A-24

I

inbound packet filtering, 1-12
Inbound Packet Filtering parameter, A-5
Init File parameter, 3-3
Input IP Address parameter, A-11
interface
  parameters
    Administrative State, A-17
    Enable ATM Signaling, A-19
    Use Hardware MAC Address, A-18
  window sequence, A-17
Interface attributes
  selecting, A-17
  window sequence, A-17
IP
  starting, 2-3
IP Address parameter, A-15
  IP configuration, 2-8, A-15

L

Learned Host Subnet Mask parameter, A-7
LLC/SNAP
  defined, B-6
LLC/SNAP service record, 2-7
Local Init File parameter, A-4

M

multiprotocol encapsulation, support, B-5

O

Output IP address parameter, A-12

P

parameters
  customizing, 3-1
parameters. *See* parameter name entry, 3-1
Pass Through Mode parameter, A-10
protocols
  editing, 2-7
  editing for hybrid access (nonbridging), 2-7
  enabling for
    hybrid access (nonbridging), 2-7
  service record, 2-7
PVCs, 2-5
  adding, 2-9
  and service records, B-5
  multiple per service record, B-7
  one per service record, B-8
  parameters
    Hybrid/Bridged VC, A-24
    VCI Number, A-24
    VPI Number, A-23

R

Relay Agent IP Address parameter, A-14
requirements, 3-1
RFC 1483 encapsulation, 1-2

S

secure learning method, 1-8
service attributes
  descriptions, A-19
  window sequence (PVC), A-20
service records
  adding (PVC), 2-7
  data encapsulation types for, 2-6
  defined, B-5
  parameters
    ATM Addr User Part, A-22
    Data Encapsulation Type, A-21
    Enable/Disable, A-21
  window sequence (PVCs), A-20
source-based routing, 1-9
starting
  IP, 2-3
  IP on circuitless interface, 2-4
Subnet Mask parameter, A-15
  IP configuration, 2-3, A-15
SVCs
  and service records, B-5

T

Target Name parameter, A-13
Target Server IP Address parameter, A-15
Technical Solutions Centers, xvii
Timeout Secs. parameter, A-9
to, 1-3
transmission path, defined, B-4
Transmit Bcast Addr parameter, A-16
  IP configuration, 2-3, A-16

U

UnNumbered Assoc Address parameter, A-16
  IP configuration, 2-3, A-16
unsecure learning method, 1-8
Use Hardware MAC Address
  parameter description, A-18

V

VCI Number
  parameter description, A-24
virtual channel identifier (VCI), defined, B-4
virtual channel, defined, B-4
virtual circuits. *See* PVCs or SVCs
virtual path identifier (VPI), defined, B-4
virtual path, defined, B-4
VPI Number
  parameter description, A-23